Protegiendo el Azure Active Directory
Mitigando las Principales Amenazas del Azure AD

Presentada por Antonio Alvarado,
CTO, Greenfence Security

GFS
GreenFence Security

Antonio Alvarado (@antonixp21)
https://greenfencesec.com
@greenfencesec

About

Antonio Alvarado

- **Ingeniero en Sistemas de Información (primera Generación)**
- **Magister en Seguridad Informática y egresado de la Universidad Tecnológica de Panamá (UTP).**

GFS
GreenFence Security

Temas

PRINCIPALES ATAQUES/TÉCNICAS

Principales ataques contra el Azure Active Directory.

CONTROLES DE SEGURIDAD PARA MITIGARLOS

Controles de seguridad para mitigar los ataques y problemas comunes en el Azure Active Directory

DEMO:EVALUACIONES DE SEGURIDAD

Demo que muestra el uso de herramientas para realizar evaluaciones de seguridad para detectar compromisos al Azure Active Directory.

GFS
GreenFence Security

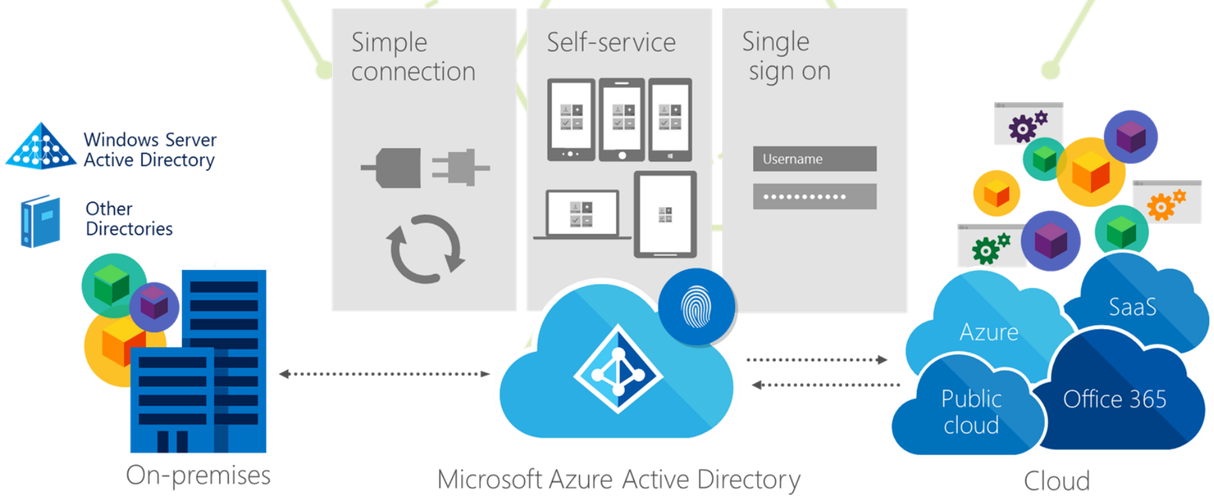
Objetivo

¿QUÉ ESPERAR?

Compartir información sobre cómo son atacados entornos integrados de Active Directory en premisas y Azure Active Directory en la nube.

GFS
GreenFence Security

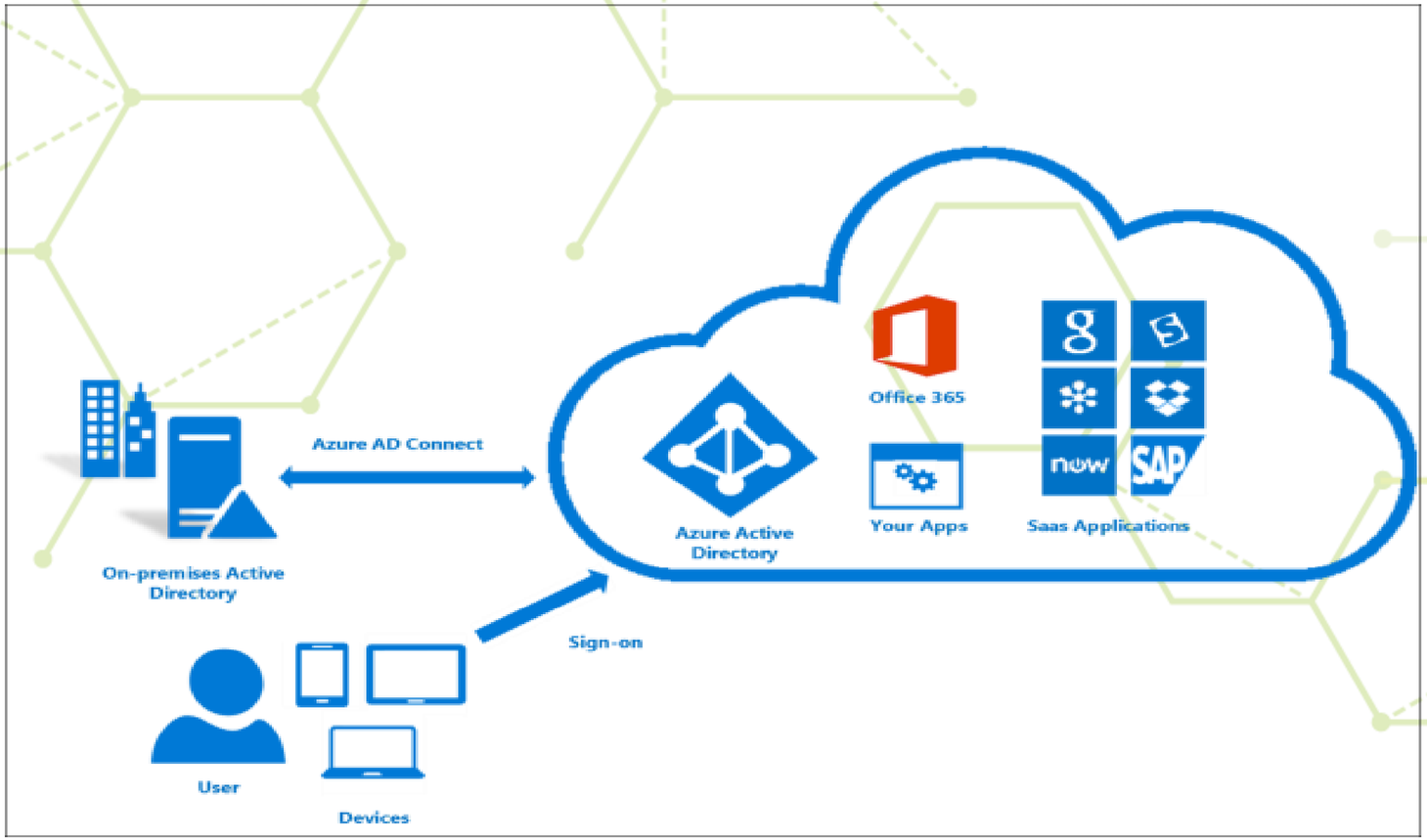
¿Qué es Azure Active Directory?



- Microsoft Azure Active Directory (Azure AD) es el servicio en la nube de Microsoft que proporciona administración de identidad y acceso.
- Proporciona la capacidad de administrar las identidades de los usuarios y los derechos de acceso.
- Azure AD combina servicios básicos de directorio, administración de acceso y protección de identidad en una única solución.
- Azure AD permite a los usuarios iniciar sesión y acceder a los recursos que se encuentran en recursos externos como Office 365 y miles de otras aplicaciones SaaS.
- También permite a sus usuarios acceder a recursos internos, como aplicaciones en la red interna de sus organizaciones.

GFS
GreenFence Security

¿Cómo se integran la tierra y la nube?



GFS
GreenFence Security

Principales Ataques

Resumen de ataques que estaremos viendo

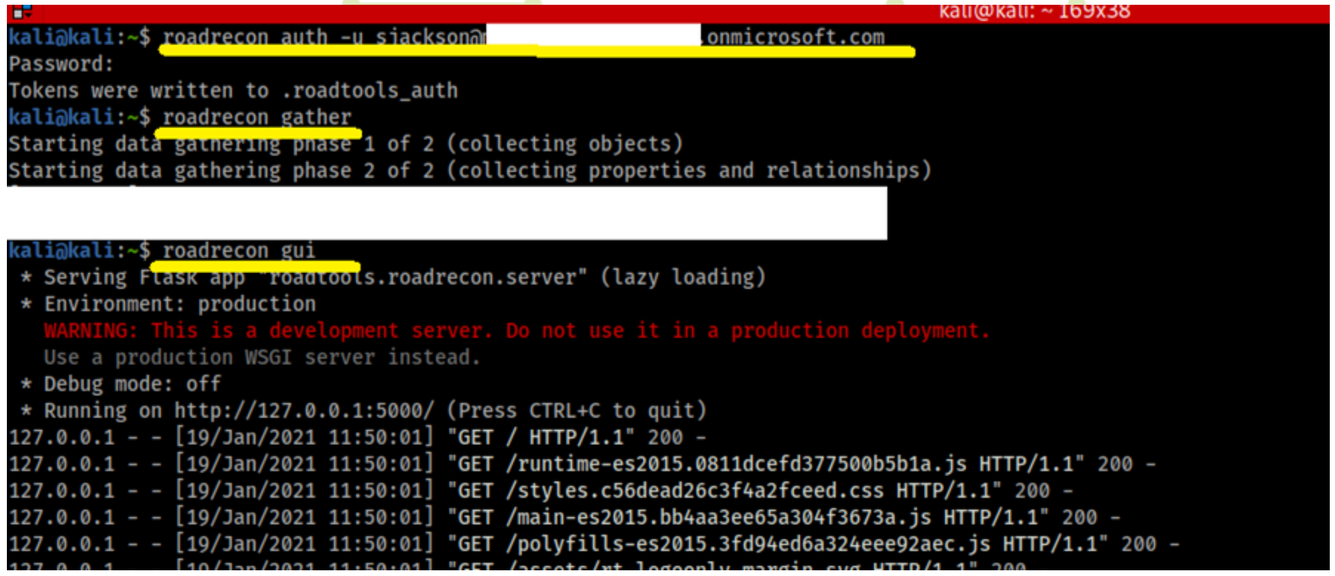
- Ataques de Reconocimiento.
- Ataques para Saltarse Segundo Factor Autenticación (MFA Bypass)
- Ataques de Phishing
- Ataques de Fuerza Bruta (Password Spray)
- Ataques al Azure AD Connect (Backdoors)
- Extracción de contraseña de Azure AD Connect

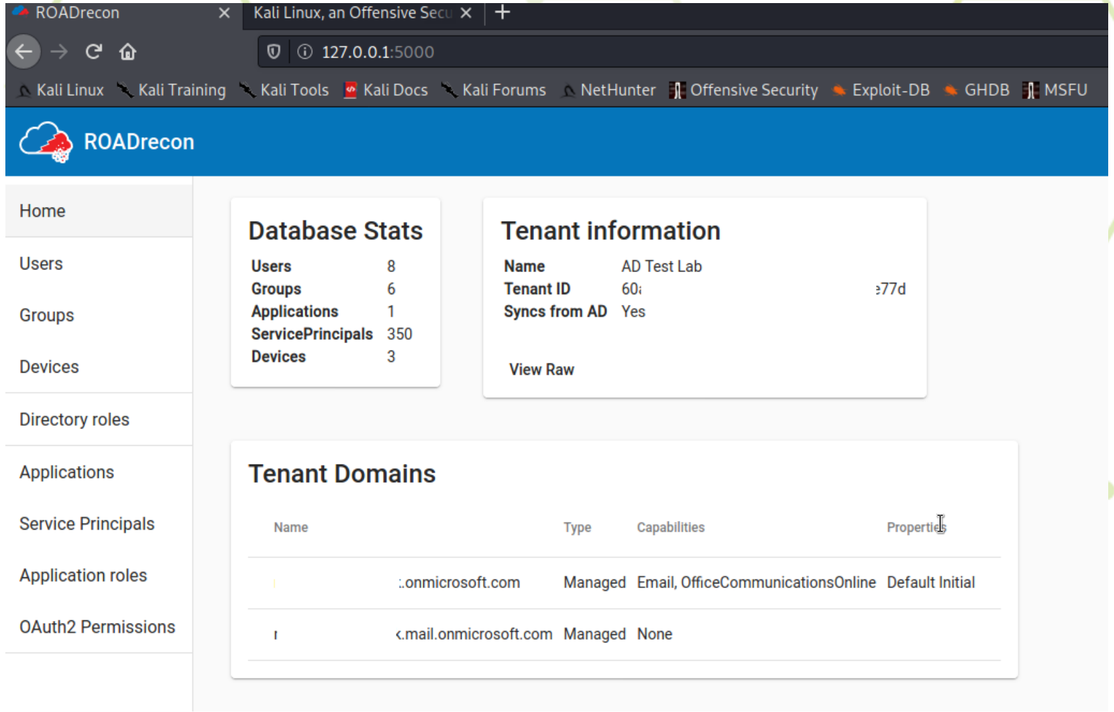
GFS
GreenFence Security

Ataques de Enumeración

Herramienta: ROADtools

Enlace: https://github.com/dirkjanm/ROADtools
Autor: Dirk-jan Mollema
Características: Recopila y muestra data de usuarios, grupos, Miembros de roles administrativos, aplicaciones, dispositivos y otros en Azure.



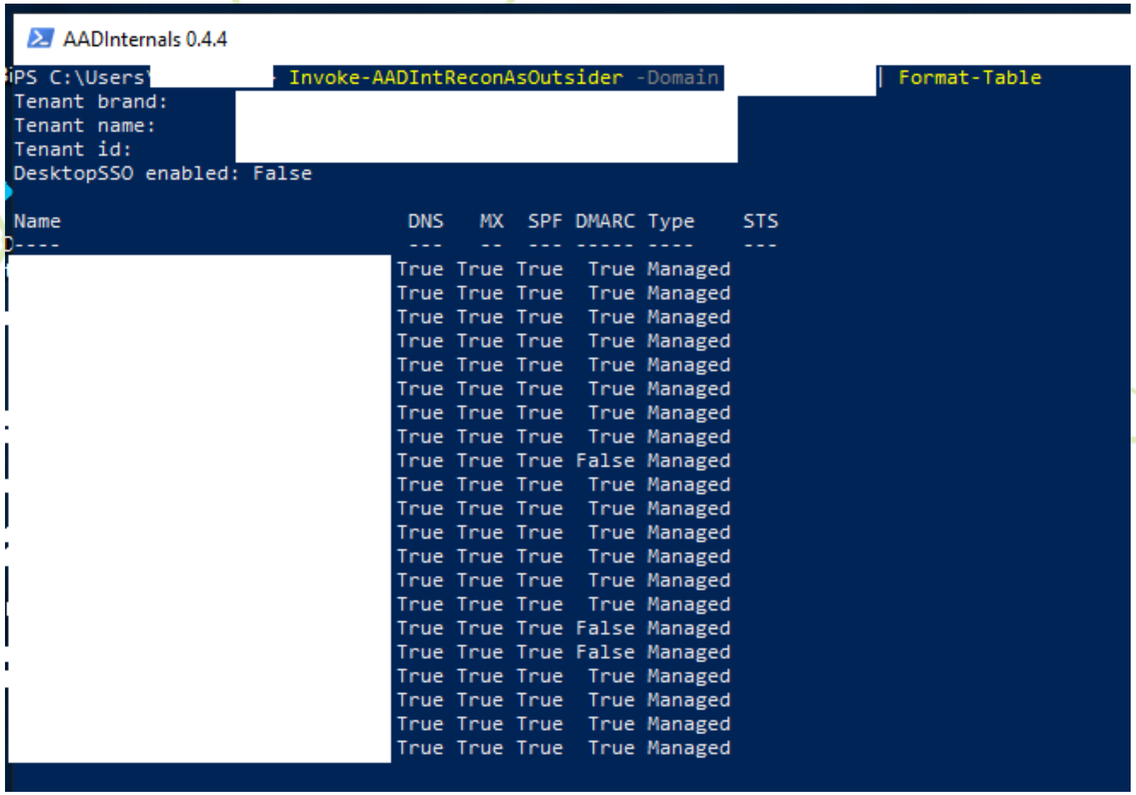


GFS
GreenFence Security

Ataques de Enumeración

Herramienta: AAD Internals

Enlace: ***https://github.com/Gerenios/AADInternals***
Autor: Dr Nestori Syynimaa
Características: Módulo de PowerShell que contiene herramientas para administrar y hackear Azure AD y Office 365.



GFS
GreenFence Security

Ataques de Enumeración

Herramienta: O365 Recon

Enlace: *https://github.com/nyxgeek/o365recon*
Autor: Nyxgeek
Características: Encuentra información de la empresa (dirección, etc.); Información de dominio (otros dominios; Lista de usuarios completa; Lista completa de grupos; Membresía grupal para cada grupo

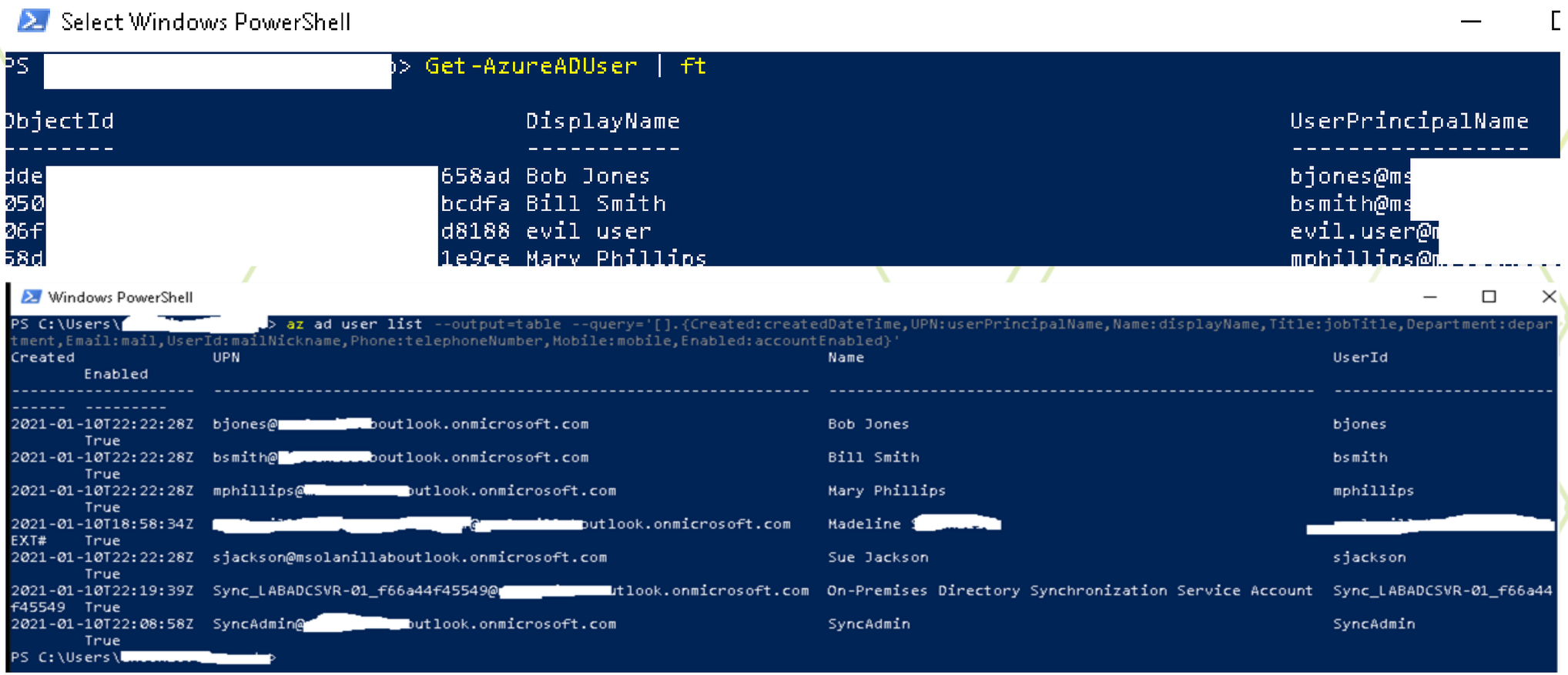
```
PS C:\Users\[redacted]> .\o365recon.ps1 -outputfile adrecon_targets
Running the -all flag
adrecon_targets


    Directory: C:\Users\[redacted]


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         1/15/2021   7:00 PM                adrecon_targets
Retrieving Company Info:

ExtensionData                           : System.Runtime.Serialization.ExtensionDataObject
AllowAdHocSubscriptions                 : True
AllowEmailVerifiedUsers                 : True
AuthorizedServiceInstances              : {MultiFactorService/NA001, Adallom/Prod05, AADPremiumService/NA001, exchan
namprd08-006-01...}
AuthorizedServices                      : {}
City                                    :
CompanyDeletionStartTime                :
CompanyTags                             : {azure.microsoft.com/azure=active}
CompanyType                             : CompanyTenant
CompassEnabled                          :
Country                                 :
```

GFS
GreenFence Security

Ataques de Enumeración

Herramienta: Azure CLI

Enlace: https://docs.microsoft.com/en-us/cli/azure/install-azure-cli
Autor: Microsoft
Características: Herramienta nativa de Microsoft para la administración de Azure.

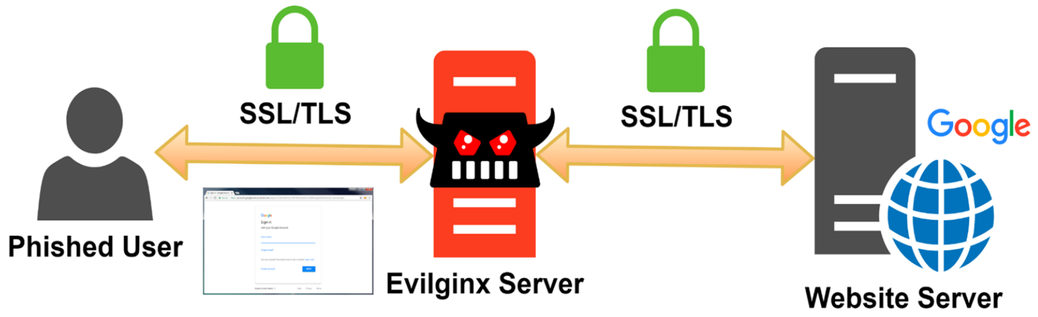


GFS
GreenFence Security

Evitar Segundo Factor de Autenticación

Herramienta: Evilginx2

Enlace: https://github.com/kgretzky/evilginx2
Autor: Kgretzky
Características: Standalone man-in-the-middle attack framework used for phishing login credentials along with session cookies, allowing for the bypass of 2-factor authentication



GFS
GreenFence Security

Evitar Segundo Factor de Autenticación

Otras Herramientas

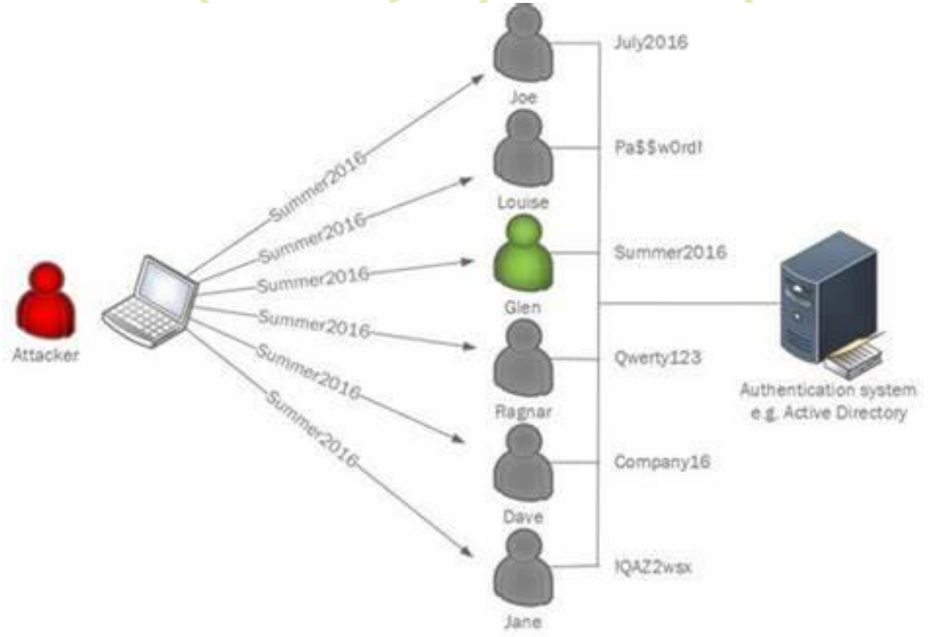
- ***AAD Internals***
- ***Modlishka***

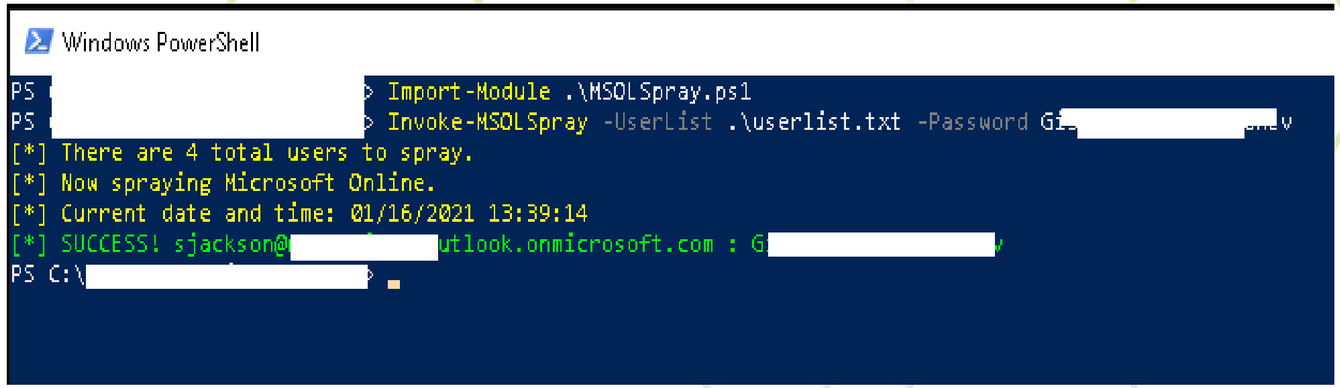
GFS
GreenFence Security

Ataque de Fuerza Bruta

Herramienta: MSOLSpray

Enlace: https://github.com/dafthack/MSOLSpray
Autor: Dafthack
Características: Permiten probar la misma contraseña sobre un grupo de usuario así evitando bloquear los usuarios.





GFS
GreenFence Security

Ataques de Fuerza Bruta

Otras Herramientas

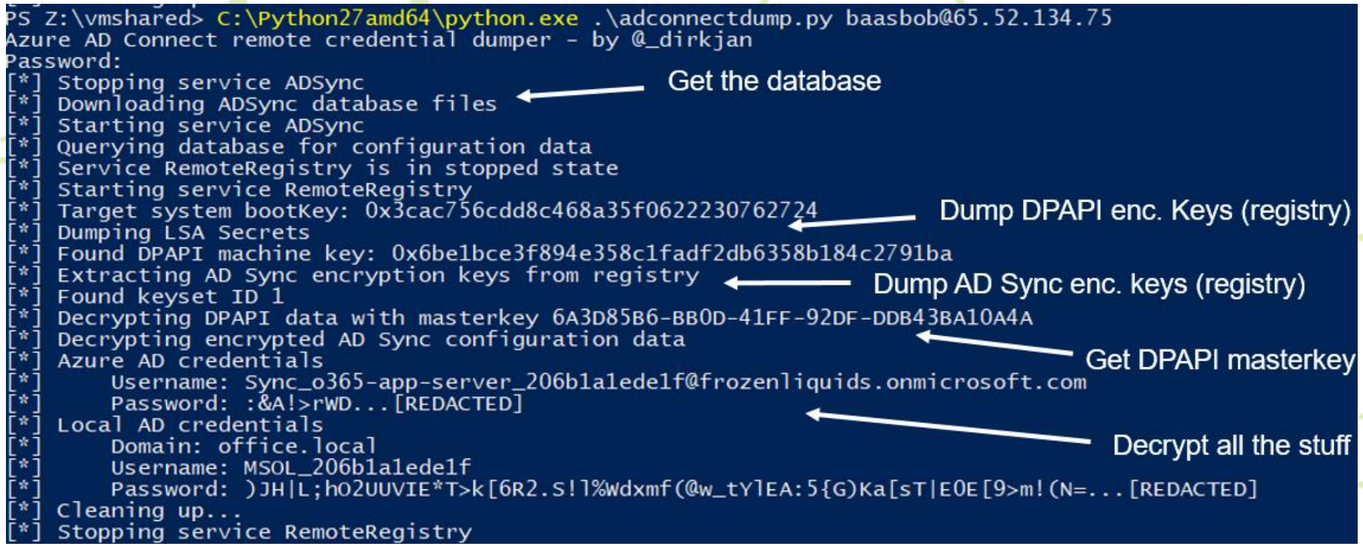
- ***MailSniper***
- ***SprayingToolkit (atomizer)***
- ***Ruler***

GFS
GreenFence Security

Ataques al AD Connect

Herramienta: ADConnectDump.py

Enlace: ***https://github.com/fox-it/adconnectdump***
Autor: Fox-IT
Características: Extrae credenciales de un servidor con servicio AD Connect instalado.

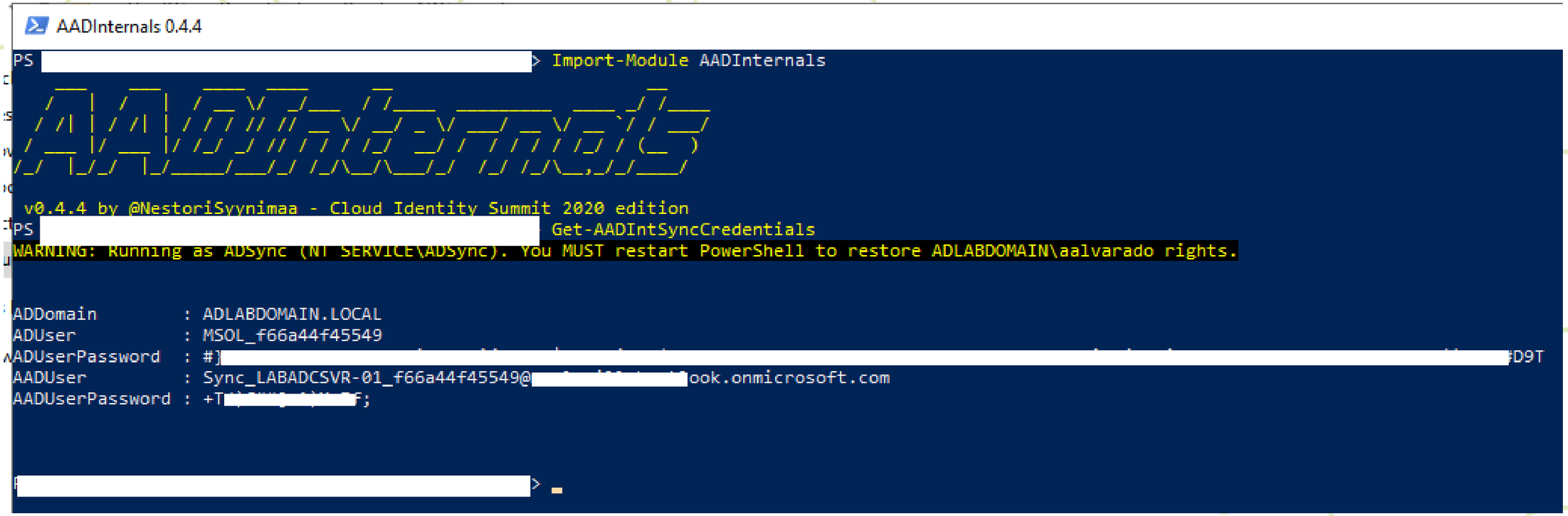


GFS
GreenFence Security

Ataques al AD Connect

Otras Herramientas

- ***AAD Internals***
- ***Mimikatz***



GreenFence Security

Ataques al AD Connect - Backdoors

Herramienta: AAD Internals

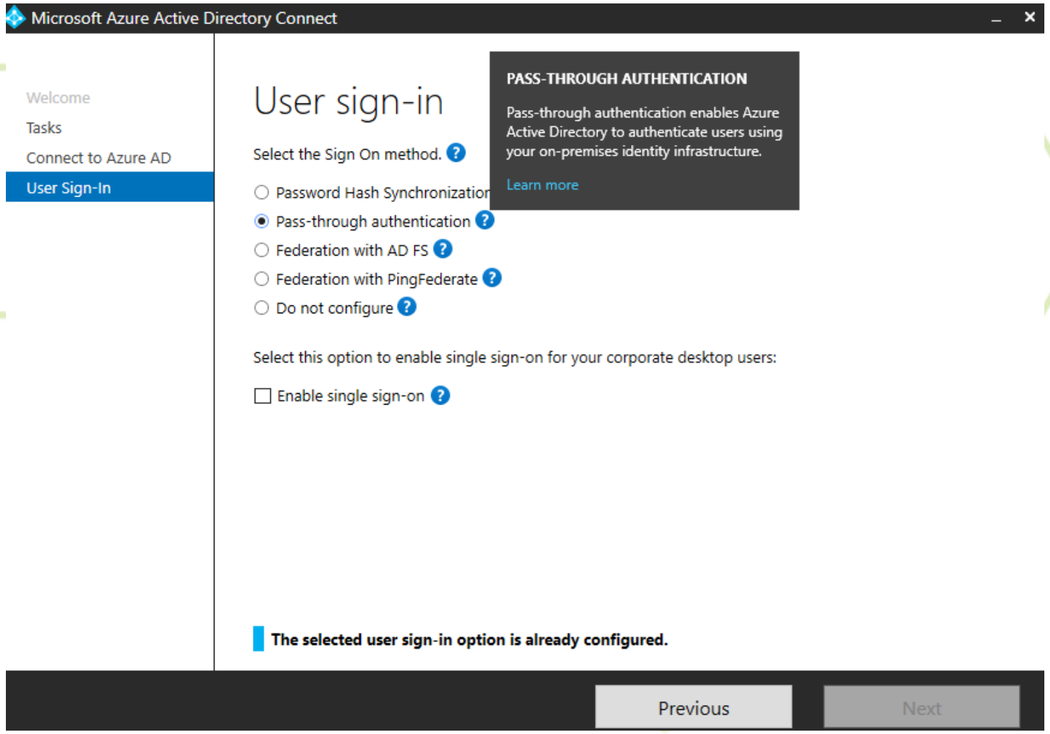
Enlace: *https://github.com/Gerenios/AADInternals*

Autor: Dr Nestori Syynimaa

Características: Instala un backdoor en el servidor AD Connect que permite recolectar todas las credenciales y las almacena en un archivo csv.

```
PS C:\Users\bhusa.BLACKHAT> Import-Module aadinternals

PS C:\Users\bhusa.BLACKHAT> whoami
blackhat\bhusa

PS C:\Users\bhusa.BLACKHAT> Install-AADIntPTASpy
WARNING: Microsoft Visual C++ 2015 Redistributable (x64) seems not to be installed! I
f PTASpy installation fails, install from: https://download.microsoft.com/download/6/
A/A/6AA4EDFF-645B-48C5-81CC-ED5963AEAD48/vc_redist.x64.exe
Are you sure you wan't to install PTASpy to this computer? Type YES to continue or CT
RL+C to abort: yes
Installation successfully completed!
All passwords are now accepted and credentials collected to C:\PTASpy\PTASpy.csv

PS C:\Users\bhusa.BLACKHAT> |
```

```
PS C:\Users\Administrator> Get-AADIntPTASpyLog -DecodePasswords

UserName                Password        Time
--------                --------        ----
garth.barks@b           sadffdsaf       6/20/2020 4:03:09 AM
garth.barks@b           sadffdsaf       6/20/2020 4:03:11 AM
garth.barks@b           ThisIsMyOnPremPW 6/20/2020 4:14:53 AM


PS C:\Users\Administrator>
```

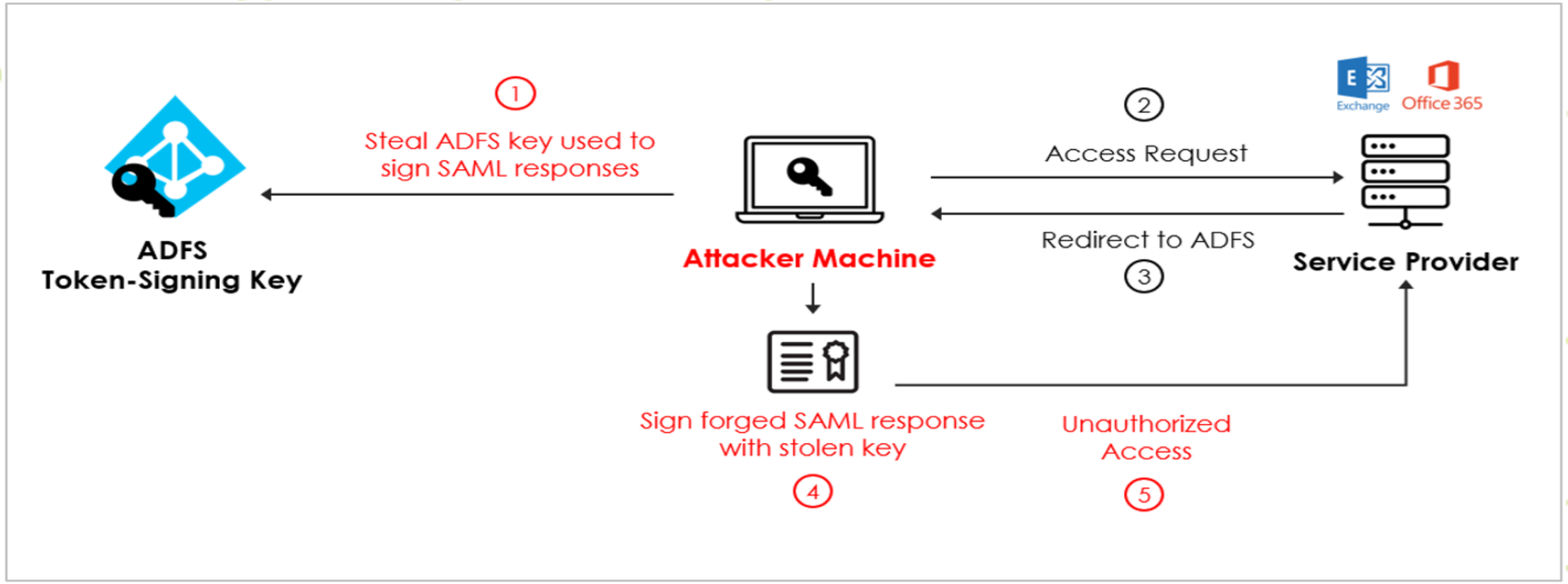


GFS
GreenFence Security

Ataques al AD Connect - Golden SAML

Herramienta: AAD Internals

Enlace: ***https://github.com/Gerenios/AADInternals***
Autor: Dr Nestori Syynimaa
Características: Exporta el certificado utilizados por los servidores de federación utilizados para firmar los token y descifrar los token de autenticación.

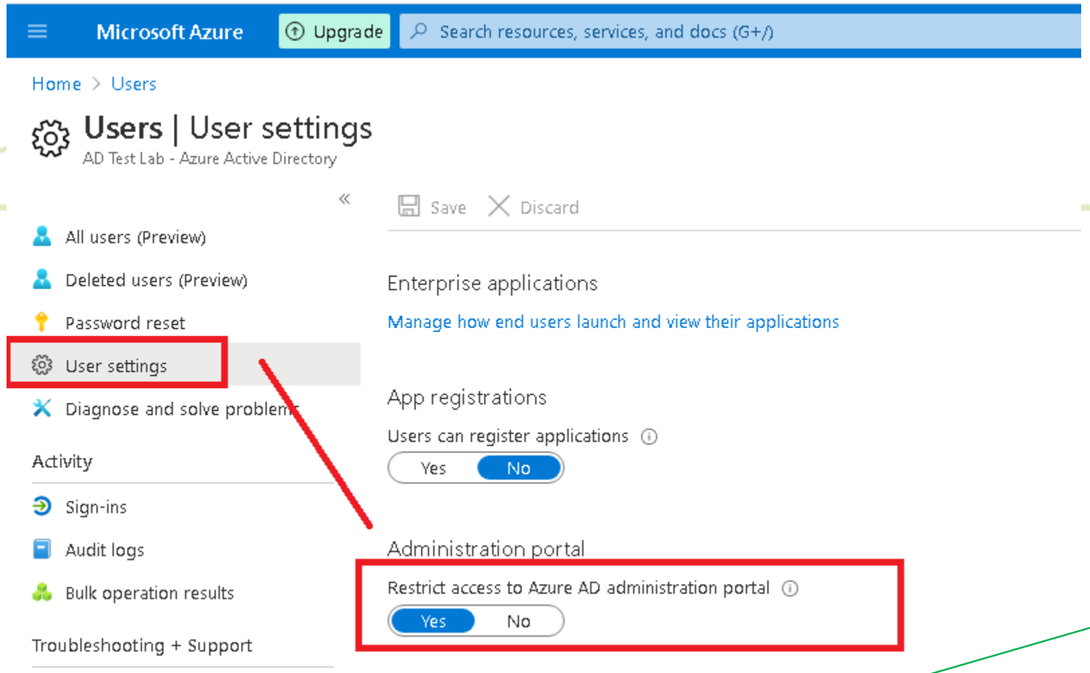


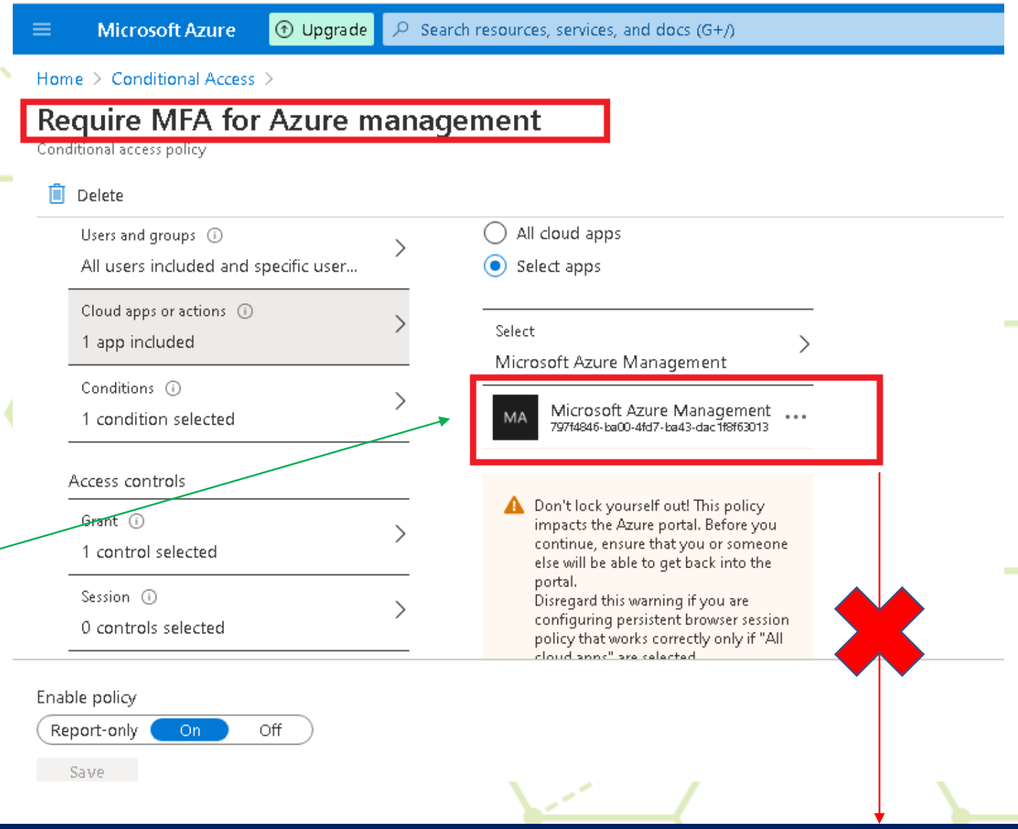
GFS
GreenFence Security

Controles de seguridad para Mitigarlos

Principales Controles de seguridad para mitigar los ataques comunes

Mitigación a Ataques de Enumeración



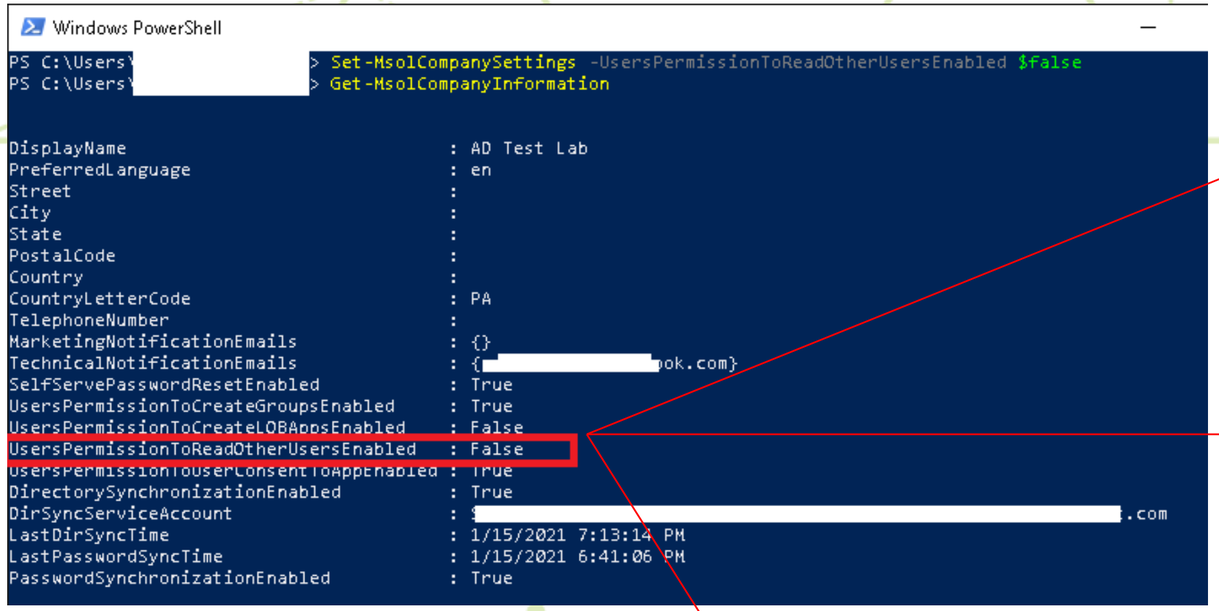


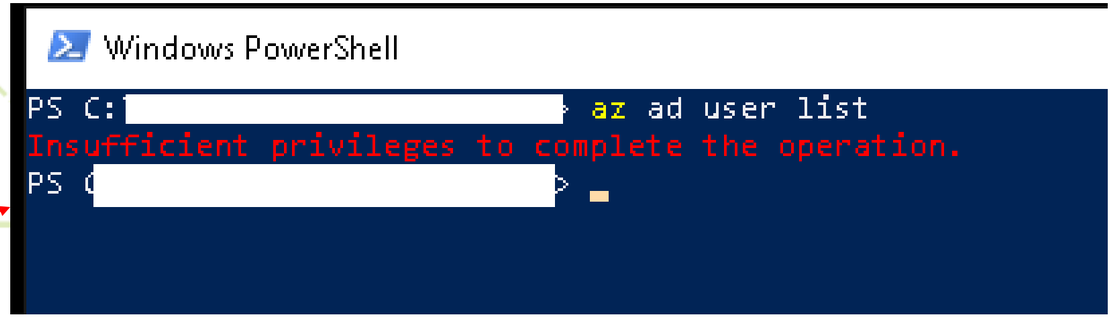
Azure portal
Azure Resource Manager provider
Classic deployment model APIs
Azure PowerShell
Azure CLI
Visual Studio subscriptions administrator portal
Azure DevOps
Azure Data Factory portal

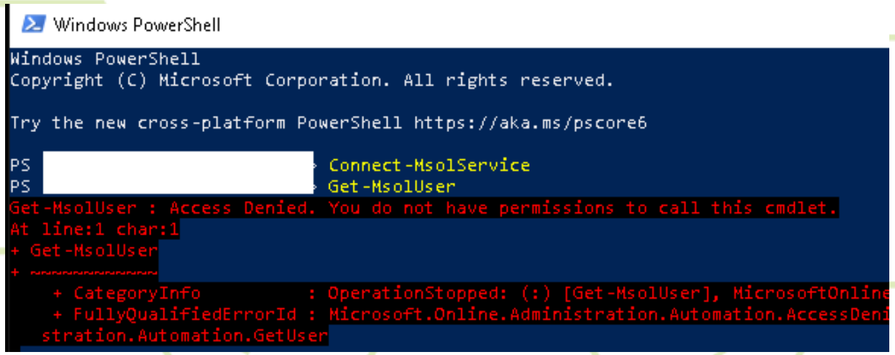
Azure Active Directory PowerShell for Graph module (AzureAD)
Microsoft Azure Active Directory Module for Windows PowerShell module (MSOnline)

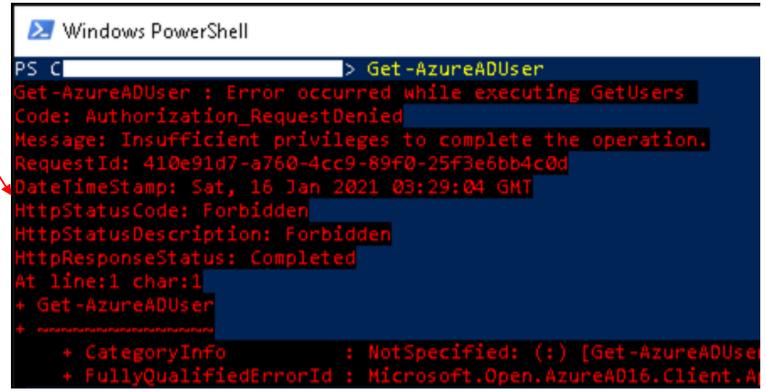
GFS
GreenFence Security

Mitigación a Ataques de Enumeración









GFS
GreenFence Security

Mitigación a Ataques de Saltarse MFA

- Educar a sus usuarios sobre la seguridad de la información y el phishing.
- Exigir a los usuarios que realicen MFA
- Política de acceso condicional en conjunto con Intune.
  - IP Fence, Hybrid Domain Join, Device Enrollment into Intune or Windows 10 Compliance Checking
- Política basada en riesgos (Azure Identity Protection)
- Custom Branding
- FIDO2/U2F (Ex: Yubico) para cuentas privilegiadas

GFS
GreenFence Security

Mitigación a Ataques de Fuerza Bruta

- Implementar políticas de contraseñas robustas. (Password Guidance)
- Forzar el uso de MFA para todas las aplicaciones en la nube.
- Configurar Azure Active Directory Password Protection
  - Smart Lockout
  - Banned passwords for cloud changes
  - Banned passwords for on-premises changes
- Block legacy authentication
- Implementar políticas de riesgo de usuario e inicio de sesión mediante (Azure Identity Protection)

GFS
GreenFence Security

Mitigación a Ataques al Servidor AD Connect

- Convertir la cuenta de servicio de AD Connect en gMSA
  - Contraseñas administradas por AD
- Limitar o restringir el acceso a los servidores Azure AD Connect.
  - Manejar los servidores AD Connect como activos de Nivel 0 (como un controlador de dominio).
- Configurar auditoría avanzada en los AD Connect.
- Implementar alertas de monitoreo para detectar manipulación de DPAPI
- Mantener actualizado el AD Connect a la última versión disponible estable.
- Implementar Hardening de Windows server para los servidores AD Connect.

GFS
GreenFence Security

Mitigación a Ataques al Servidor AD Connect

- Utilice Password hash Sync en lugar de la autenticación Pass-Through Authentication.
- Enviar todos los registros de auditoría unificados de O365 y los registros de Azure a un SIEM para crear detecciones de ataques.
- Periódicamente ejecutar las evaluaciones de detección de compromisos de tipo backdoors como lo son las siguientes:
  - CISA's Sparrow,
  - Open-source utility Hawk, and
  - CrowdStrike's Azure Reporting Tool (CRT).
- Limitar las cuentas que se sincronizan.
- No sincronizar cuentas privilegiadas ni de servicios en la nube de Azure.

GFS
GreenFence Security

Mitigación a Ataques al Servidor AD Connect

- Utilice Password hash Sync en lugar de la autenticación Pass-Through Authentication.
- Enviar todos los registros de auditoría unificados de O365 y los registros de Azure a un SIEM para crear detecciones de ataques.
- Periódicamente ejecutar las evaluaciones de detección de compromisos de tipo backdoors como lo son las siguientes:
  - CISA's Sparrow,
  - Open-source utility Hawk, and
  - CrowdStrike's Azure Reporting Tool (CRT).
- Limitar las cuentas que se sincronizan.
- No sincronizar cuentas privilegiadas ni de servicios en la nube de Azure.

GFS
GreenFence Security

Lista de Verificación de Mitigaciones por Ataques

Ataques de Reconocimiento.
☐Restringir o bloquear el acceso a los portales administrativos a usuarios no administrativos.
☐Restringir el acceso a portales administrativos mediante acceso condicional.
☐Restringir el acceso de lectura por defecto de usuarios estándar mediante **Set-MsolCompanySettings**
Ataques para Saltarse Segundo Factor Autenticación (MFA Bypass)
☐Política de acceso condicional en conjunto con Intune.
IP Fence, Hybrid Domain Join, Device Enrollment into Intune or Windows 10 Compliance Checking
☐Política basada en riesgos (Azure Identity Protection)
☐Custom Branding
☐FIDO2/U2F (Ex: Yubico) para cuentas privilegiadas
Ataques de Phishing
☐Educar a sus usuarios sobre la seguridad de la información y el phishing.
☐Custom Branding
☐Política basada en riesgos (Azure Identity Protection)
☐Audite los permisos consentidos para las aplicaciones y el acceso de los usuarios a las aplicaciones.
☐Revisar los permisos de la aplicación
☐Supervisar los registros de aplicaciones.

GFS
GreenFence Security

Lista de Verificación de Mitigaciones por Ataques

Ataques de Fuerza Bruta (Password Spray)
☐Implementar políticas de contraseña robustas. (Password Guidance)
☐FIDO para cuentas privilegiadas.
☐Forzar el uso de MFA para todas las aplicaciones en la nube.
☐Habilite MFA para todos los usuarios a través del acceso condicional o en políticas de riesgos de (Azure Identity Protection).
☐Deshabilitar la autenticación heredada (Block Legacy Authentication) por completo a través del acceso condicional.
☐Habilite el restablecimiento de contraseña mediante autoservicio (SSPR).
☐Configurar Azure Active Directory Password Protection
○ Smart Lockout
○ Banned passwords for cloud changes
○ Banned passwords for on-premises changes
☐Habilitar Azure AD Connect Health para ADFS y ADFS Smart Lockout
☐Implementar políticas de riesgo de usuario e inicio de sesión mediante (Azure Identity Protection)
☐Recoleta y enviar los eventos de Azure AD a un SIEM o utilice Azure Log Analytics o Azure Sentinel

GFS
GreenFence Security

Lista de Verificación de Mitigaciones por Ataques

Ataques al Azure AD Connect (Backdoors)
☐Limitar o restringir el acceso a los servidores Azure AD Connect.
☐Solicitar MFA para todas las cuentas privilegiadas de la nube.
☐Configurar PIM para todas las cuentas privilegiadas de la nube.
☐Manejar los servidores AD Connect como activos de Nivel 0 (como un controlador de dominio).
☐Cree cuentas de administrador global dedicadas independientes.
☐Las cuentas de administradores Globales solo deben existir en la nube no deben ser cuentas sincronizadas de su premisa.
☐Utilice Password hash Sync en lugar de la autenticación Pass-Through Authentication.
☐Envié todos los registros de auditoría unificados de O365 y los registros de Azure a un SIEM para crear detecciones de ataques.
☐Periódicamente ejecutar las evaluaciones de detección de compromisos de tipo backdoors como lo son las siguientes:
○ CISA's Sparrow,
○ Open-source utility Hawk, and
○ CrowdStrike's Azure Reporting Tool (CRT).
☐Limitar las cuentas que se sincronizan.
☐FIDO para cuentas privilegiadas.
☐No sincronizar cuentas privilegiadas ni de servicios en la nube de Azure.
☐Recoleta y enviar los eventos de Azure AD a un SIEM o utilice Azure Log Analytics o Azure Sentinel

GFS
GreenFence Security

Lista de Verificación de Mitigaciones por Ataques

Extracción de contraseña de Azure AD Connect
☐Cree alertas de monitoreo en su SIEM para detectar las herramientas utilizadas actualmente para extraer credenciales de los AD Connect:
○ AAD Internals
○ Adconnectdump
○ Mimikatz
☐Convertir la cuenta de servicio de AD Connect en gMSA
○ Contraseñas administradas por Active Directory
☐Limitar o restringir el acceso a los servidores Azure AD Connect.
☐Manejar los servidores AD Connect como activos de Nivel 0 (como un controlador de dominio).
☐Configurar auditoría avanzada de eventos de seguridad en los AD Connect.
☐Implementar alertas de monitoreo para detectar manipulación de DPAPI
☐Mantener actualizado el AD Connect a la última versión disponible estable.
☐Implementar Hardening de Windows server para los servidores AD Connect.
☐Recoleta y enviar los eventos de Azure AD a un SIEM o utilice Azure Log Analytics o Azure Sentinel

GFS
GreenFence Security

GFS
GreenFence Security

DEMO

Demo: Herramientas de Evaluaciones de seguridad de Azure Active Directory

GitHub (Antonixp21)

antonixp

antonio-aac

GFS
GreenFence Security